UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA v. ANDREW OTTO BOGGS (a/k/a "INCURSIO") Defendant.	Criminal No. 1:16-cr-314 Honorable Gerald Bruce Lee Sentencing: June 30, 2017

GOVERNMENT'S POSITION ON SENTENCING

Defendant Andrew Otto Boggs has pleaded guilty to conspiring with Justin Liverman[1] and others to commit identity theft and unauthorized access to a protected computer. His conviction stems from his conduct in 2015 and 2016 with an online collective – calling itself "Crackas with Attitude" or CWA – that targeted U.S. government personnel for harassment and unauthorized account intrusions. The plea agreement stipulates that defendant's adjusted offense level under the U.S. Sentencing Guidelines is 16, resulting in a sentencing range of 21-27 months. The Presentence Investigation Report (PSR) agrees with this calculation. The government submits that under the factors in 18 U.S.C. § 3553(a), a sentence at the low end of this guidelines range would be sufficient but not more than necessary to meet the objectives in that statute. The government further requests that the Court order three years of supervised release and full restitution that imposes joint and several liability on co-conspirator Liverman, who will be sentenced next month.

[1] Case No. 1:16-CR-313-GBL (E.D. Va.).

SENTENCING ANALYSIS

Earlier this year, defendant pleaded guilty to one count of conspiracy to commit identity theft (a violation of 18 U.S.C. § 1028) and unauthorized access to a protected computer (a violation of 18 U.S.C. § 1030), all in violation of 18 U.S.C. § 371. PSR ¶ 3. The maximum penalties for this crime are 5 years' imprisonment, a $250,000 fine, and 3 years of supervised release. Defendant has also agreed to pay full restitution and a $100 special assessment. A forfeiture order was entered at defendant's plea hearing.

The Sentencing Guidelines and the factors in 18 U.S.C. § 3553(a) govern the Court's sentencing analysis. While the Guidelines have been advisory since 2005, district courts are required to "consult those Guidelines and take them into account when sentencing." *United States v. Booker*, 543 U.S. 220, 264 (2005). Indeed, the continued use of the Guidelines as a benchmark helps to avoid unwarranted sentencing disparities. After calculating the appropriate sentencing range, "the court shall consider that range as well as other relevant factors set forth in the guidelines and those factors set forth in [18 U.S.C.] § 3553(a) before imposing the sentence." *United States v. Hughes*, 401 F.3d 540, 546 (4th Cir. 2005) (citation omitted).

I. Sentencing Guidelines

The plea agreement in this case stipulates that the following Guidelines apply:

Base offense level (Section 2B1.1(a)(2))	6
Amount of loss attributable to defendant under 18 U.S.C. § 3664(h) is more than $95,000 but not more than $150,000 (Section 2B1.1(b)(1)(E)	+8
Substantial part of a fraudulent scheme was committed from outside of the United States; and/or the offense involved sophisticated means (Section 2B1.1(b)(10))	+2
A victim of the offense was a government officer or employee (Section 3A1.2(a))	+3

Acceptance of responsibility (Section 3E1.1)	-3
Total Offense Level	**16**

Given defendant's timely acceptance of responsibility, the government moves the Court for a one-level reduction under U.S.S.G. § 3E1.1(b), as reflected in the chart above, which the Probation Office has appropriately included in its calculations. PSR ¶ 49. The PSR's assessment of defendant's offense level mirrors the parties' above stipulation. With defendant's criminal history category of 1, the resulting sentencing range is 21-27 months' imprisonment.

II. Section 3553(a) Factors

Applying the factors in 18 U.S.C. § 3553(a), the government submits that a sentence at the low end of defendant's guidelines range is appropriate, particularly given the nature and circumstances of the offense; defendant's relative role in the conspiracy; and the need for the sentence to reflect the seriousness of the offense, promote respect for the law, and afford adequate deterrence.

There is no dispute about the serious nature of defendant's offense. From around July 2015 to April 2016, defendant conspired with others to break into U.S. government officials' online accounts and law enforcement databases. The group's objectives were to harass, pilfer law enforcement data to post online, and seek self-glory. Defendant and his co-conspirators crowed on Twitter of their exploits while hopscotching between victims in the fall and winter. They shared unlawfully obtained law enforcement information with online journalists who wrote about CWA. PSR Ex. 1 at 11. Their motives, in short, were in equal measure wreaking havoc and self-aggrandizement. In total, defendant and his co-conspirators targeted more than 10 victims and caused more than $1.5 million in losses. Statement of Facts (SOF)[2] ¶ 2.

[2] ECF No. 52; text reproduced in PSR ¶ 28.

Defendant's activity with the criminal conspiracy was less extensive than Liverman's, who selected some of the group's victims and who initiated his own harassment campaigns in some instances. PSR ¶ 35. But defendant was dedicated to the group's objectives and to the group's leader, a U.K.-based hacker in his mid-teens who went by "Cracka." *Id.*

In spring 2015, defendant, who had met Cracka online, encouraged Cracka to engage in social engineering to gain unauthorized computer access. SOF ¶ 4, PSR ¶ 11. Then in July 2015, after learning that Cracka had recently hacked into a high-profile victim's email account, defendant broached the idea of joining forces. In a series of private Twitter messages, defendant asked whether Cracka would be interested in joining a hacking group that would target only "governments and security firms." SOF ¶ 5, PSR ¶ 11. In a description of the group he sent Cracka, defendant stated that he was "planning to start launching attacks under TeamInnocuous after recruitment is done." Similarly, in a message to Cracka, defendant wrote, "I'm waiting on our logo to be finished before we commence attacks on governments." Cracka replied, "Sure, I'd love to join." SOF ¶ 5.

In fall 2015, Cracka used social engineering to break into Victim 1's personal online accounts, and then sent defendant Victim 1's personal email address and identifying information. PSR ¶ 14. Defendant told Cracka that he was going to help him "own" Victim 1's government agency (*id.*), and several days later offered his assistance to Cracka "with whatever [h]e c[ould] help with." ECF No. 2 ¶ 21. Around this time in October 2015, Victim 1 received multiple harassing phone calls at his home and on his cellphone from members of the conspiracy. PSR ¶ 14. The Sentencing Guidelines recognize an "official victim" enhancement in part due to the crime's "potential disruption of the governmental function" (U.S.S.G. § 3A1.2 note 5), and no less with Victim 1 did this apply, as government resources had to be diverted to deal with the conspirators. PSR ¶ 19.

In November 2015, after learning that Cracka had gained unlawful access to Victim 2's online account, defendant expressed his desire to "get involved with hacking and programming for CWA." SOF ¶ 12. Later, defendant and Cracka both used Victim 2's official credentials to break into a law enforcement database used by government intelligence groups and criminal justice entities. PSR ¶¶ 21, 23. Once in this database, the conspirators extracted sensitive information about the identity of other law enforcement offices in the United States, and gained access to arrest and booking records available only to law enforcement. PSR Ex. 1 at 1. Members of the conspiracy including Liverman also engaged in a weeks-long harassment campaign against Victim 2, his family, and his friends and relatives, among others. PSR ¶ 21 & Ex. 1 at 1. As with Victim 1, the conspirators' attacks on Victim 2 caused a significant diversion of government resources to investigate and deal with the conspirators. PSR ¶ 24 & Ex. 1 at 1.

Throughout the conspiracy, defendant and his co-conspirators regularly sought to enhance their online notoriety by posting information they had unlawfully obtained – with seeming no regard to any resulting consequences to their victims. In fall 2015, defendant volunteered to "publish the stolen information" Cracka had unlawfully obtained from Victim 1's accounts (SOF ¶ 9), and later he told Cracka that there was "[n]o better of protesting than hacking and leaking more documents over and over again." SOF ¶ 10. And "publish" they did. Co-conspirator Liverman posted to public websites the identities of dozens of local law enforcement personnel that Cracka obtained from a government database with Victim 2's credentials. PSR ¶ 22. In early 2016, after Cracka gained unlawful access to a U.S. Department of Justice computer system, defendant agreed to post non-public information from that system –

personnel directories that contained names and contact information for tens of thousands of Justice Department and Homeland Security Department employees. SOF ¶ 16; PSR Ex. 1 at 11. News outlets noticed – indeed, the conspirators shared documents with some online news writers. PSR Ex. 1 at 11. In February 2016, defendant posted this trove of unlawfully obtained information multiple times on multiple sites, and encouraged others to do the same. PSR ¶ 25. As noted in the victim statements, these postings "created a tangible vulnerability to the safety of government personnel" due to law enforcement identities being disclosed so publicly. PSR Ex. 1 at 1, 10.

Defendant may claim that his actions "did not seem real" to him at the time (PSR ¶ 58), but he certainly understood that they carried real consequences if he were caught. For instance, defendant suggested using public Internet connections to conceal his true whereabouts when publishing "stolen information." SOF ¶ 9. Defendant warned Cracka to take care when accessing law enforcement databases with Victim 2's credentials, as Cracka could be jailed if his identity was discovered. PSR ¶ 23. Similarly, defendant urged others online to conceal their steps when disseminating information that CWA had unlawfully obtained. PSR ¶ 25. Yet defendant chose to continue in the conspiracy. Indeed, ever after Cracka was arrested, defendant defiantly posted on his Twitter page: "Will we stop attacking governments since cracka got arrested? Simple answer: no. In fact, our campaign will only intensify now." In light of the above, the government submits that a paramount consideration for defendant's sentence is that it promotes respect for the law and sends a signal to others who might consider following his steps.[3]

[3] The government also notes that its recommended sentence would be consistent with sentences given to other computer hackers in this District, including defendant Matthew Buchanan (1:13-CR-501-TSE), who received an 18-month sentence for one count of committing unauthorized access to a computer (in that case, Google accounts). Buchanan's sentence, which was assessed

CONCLUSION

For the reasons stated above, the government respectfully submits that a sentence at the low end of the Guidelines range of 21-27 months is sufficient but not greater than necessary under 18 U.S.C. § 3553(a). The government also respectfully requests a three-year term of supervised release, as well as the entry of a restitution order for $104,145 – payable to victims whose names will be submitted under seal – to which defendant and co-defendant Liverman are jointly and severally liable.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s/
Maya D. Song
Jay V. Prabhu
Assistant United States Attorneys

Joseph V. Longobardo
Special Assistant United States Attorney (LT)

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
Tel: (703) 299-3700
Fax: (703) 299-3981
maya.song@usdoj.gov
jay.prabhu@usdoj.gov
joseph.longobardo@usdoj.gov

on an offense level 13 with zero criminal history points, was affirmed in *United States v. Buchanan*, 586 F. App'x 145 (4th Cir. 2014).

CERTIFICATE OF SERVICE

I hereby certify that on June 24, 2017, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will automatically generate a Notice of Electronic Filing to counsel of record for defendant Andrew Otto Boggs.

By: /s/

Maya D. Song
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
Ph: (703) 299-3700
Fax: (703) 299-3981
maya.song@usdoj.gov